Demo: Automatic Personal Identification System for Security in Critical Services: A Case Study

Stefano Tennina, Marco Di Renzo, Luigi Luigipomante, Roberto Alesii, Fortunato Santucci, Fabio Graziosi

Demo: Automatic Personal Identification System for Security in Critical Services - A Case Study

Stefano Tennina
CISTER Research Center
Polytechnic Institute of Porto (ISEP/IPP)
Porto, Portugal
sota@isep.ipp.pt

Marco Di Renzo
Laboratory of Signals and Systems (L2S)
UMR 8506 CNRS - SUPELEC
Paris, France
marco.direnzo@lss.supelec.fr

Luigi Pomante
Center of Excellence DEWS
University of L'Aquila
L'Aquila, Italy
luigi.pomante@univaq.it

Roberto Alesii
Center of Excellence DEWS
University of L'Aquila
L'Aquila, Italy
roberto.alesii@univaq.it

Fortunato Santucci
Center of Excellence DEWS
University of L'Aquila
L'Aquila, Italy
fortunato.santucci@univaq.it

Fabio Graziosi
Center of Excellence DEWS
University of L'Aquila
L'Aquila, Italy
fabio.graziosi@univaq.it

Abstract

The demonstration proposal moves from the capabilities of a wireless biometric badge [4], which integrates a localization and tracking service along with an automatic personal identification mechanism, to show how a full system architecture is devised to enable the control of physical accesses to restricted areas. The system leverages on the availability of a novel IEEE 802.15.4/Zigbee Cluster Tree network model, on enhanced security levels and on the respect of all the users' privacy issues.

Categories and Subject Descriptors

C.2.1 [**Computer-Communication Networks**]: Network Architecture and Design—*Wireless communication*

General Terms

Experimentation

Keywords

WSN, Biometric, Personal Identification

1 Introduction

The relevant innovations in the ICT domain enable new services for a growing number of people with the intent of simplifying the tasks of every day's life (e.g., cash retrieval, remote-banking, etc.). The key aspect to fully enable such services and make them widely accepted is the possibility to reliably count on biometric identification mechanisms [1]. Although some of them are already available, they are still widely exposed to the risk of malicious operations. Hence, the best way to support the evolution of automatic services is to develop a (automatic) system, able to check the users' identity. The success of such systems depends on their easy integration in different scenarios, especially when an existing infrastructure is already in-place, and on a design focused on the respect of all the relevant privacy issues, but flexible enough to provide the users with the feeling (i.e., reliability, safety and usability) needed to make the system accepted.

In such a context, WEST Aquila [6] recently presented [4] an automatic personal identification system, which exploits the recent advances in the biometric and heterogeneous wireless networks fields to provide a true authentication platform able to support several services, including physical access (e.g., to restricted areas or vehicles) as well as logical access (e.g., to personal services, like e-banking) management. The main component of the system is a novel biometric badge, i.e., a smart-card equipped with a fingerprint reader and a wireless transceiver, with which the identification of both the card itself and its owner is enabled. When required, the card's owner is identified through an on-system biometric matching and only the result of such a matching is sent (appropriately ciphered) through the wireless interface towards the rest of the system. Therefore, personal biometric data is always under the full control of its owner, leading to high levels of security and privacy protection.

2 System Architecture

The proposed architecture is sketched in Fig. 1 and is composed by a set of elements (detailed in the following) enabling the high level of flexibility and reliability needed to make it a reference in the field of personal automatic identification systems, where the emphasis is on aspects like robustness, ease-of-use and privacy.

Biometric Badge (BB). As a "system-on-badge" [4], the embedded biometric badge performs four main tasks: (i) to enable the localization of its owner using distributed positioning techniques, (ii) to scan and verify fingerprints [5],

SenSys'11, November 1–4, 2011, Seattle, WA, USA.
ACM 978-1-4503-0718-5/11/11

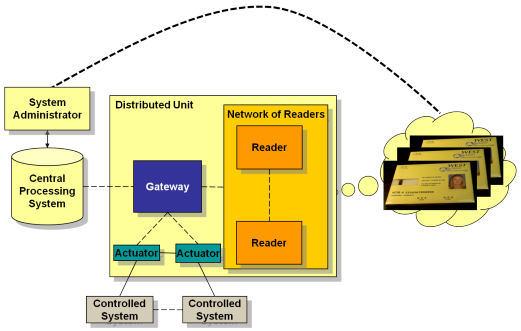

Figure 1. Logical System Architecture

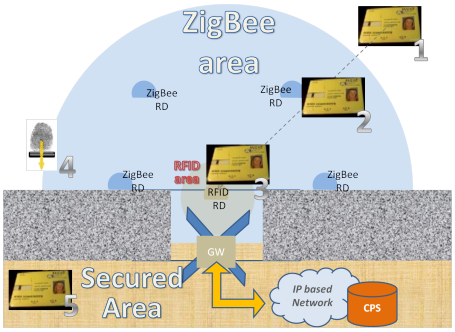

Figure 2. Case Study – Physical access to a critical area

(iii) to check if an user is the badge's owner based on fingerprint matching, and (iv) to send related outcomes to the rest of the system, without the need of transmitting owners' biometric data over the wireless medium.

Distributed Unit (DU). Every DU is logically constituted by a "Gateway" (GW), one or more "Readers" (RDs) and one or more "Actuators" (ATs) communicate over wireless or wired media. The whole system can rely on several DUs, networked over secure channels with a Central Processing Station (CPS).

Gateway (GW). It is the central element of each DU. Its main function is to provide an interface between the BBs and the CPS: (i) it collects data from BBs through its associated RDs and sends them to CPS, and (ii) receives instructions from CPS to control ATs to grant or deny the access to BBs.

Reader (RD). It is the interface between the DU and the BBs. When the communication between the RDs and the GW is wireless and multi-hop, the RDs constitute a network of readers (NRD), organized according to the ZigBee Cluster Tree model [2, 3].

Actuator (AT). It is the device in direct contact with the Controlled System and allows the GW to grant the access to the authenticated users.

Central Processing System (CPS). It contains data for the whole system configuration: it stores and handles BBs' grants with respect to the different UDs, as well as the services that BB's owners can access, once authenticated. CPS is the interface with the "System Administrator" (SA), which is in charge of (i) delivering the BBs to people, and (ii) adding/updating all system configuration data (enrollment), i.e., the association between the BBs and the services allowed to its owner.

3 Demo: Access to a Critical Area

Let us assume that a SA has released a number of BBs to authorized people. This means that each BB stores the fingerprint of its owner and the central system is aware of the access rights of each BB.

The access to a critical area towards a controlled gate is performed by means of the following steps (Fig. 2). (i) The BB is in stand-by mode, i.e., it is waiting for a beacon sent by one of the RDs forming a ZigBee Cluster Tree topology [2, 3]. (ii) When the BB enters the ZigBee area, it is able to ear the beacons sent by the RDs and to communicate with the control unit on the gate, in order to inform it about its arrival. In this context, the badge implements a positioning solution [4] modified to use the information provided within the beacon messages sent by the RDs. The DU is able to communicate with the CPS in order to make in advance any control related to the badge identification (i.e., to check if it is allowed to access the gate it is approaching). (iii) Assuming that the BB is allowed to pass the gate, the DU waits for the proximity of the BB. (iv) When the BB is close to the gate, DU asks the BB to start the personal identification, i.e., the BB asks the owner to scan his/her fingerprint, it compares that scan with the stored one, and (only) the result of such a verification is sent (ciphered) back to the DU, where the GW is the only device able to decode that information. (v) If the identification is successful, DU opens the gate, otherwise proper actions defined by the SA at system setup are taken.

4 Acknowledgments

This work has been supported by WEST Aquila srl [6]. The research activity of Stefano Tennina is supported by the EMMON project, funded by National Funds, through the FCT - Portuguese Foundation for Science and Technology (grant ref. ARTEMIS/0003/2008), as well as by the ARTEMIS Joint Undertaking (grant agreement n. 100036). The work done by Fortunato Santucci and Fabio Graziosi is supported by the FP7 NoE HYCON2, project number 257462 and project IRMA2 (Ministry of Defense of Italy).

5 References

[1] O. S. Adeoye. A survey of emerging biometric technologies. *International Journal of Computer Applications*, 9(10):1–5, November 2010.

[2] J.-H. Hauer et al. An open-source ieee 802.15.4 mac implementation for tinyos 2.1, February 2011. Poster Session at 8th European Conference on Wireless Sensor Networks.

[3] P. Jurcik et al. Dimensioning and worst-case analysis of cluster-tree sensor networks. *ACM Transactions on Sensor Networks*, 7(2), August 2010.

[4] S. Tennina et al. Integrated gps-denied localization, tracking and automatic personal identification. In *SenSys*, pages 355–356. ACM, 2009.

[5] UPEK. Chipset tcs3-tcd42, touchstrip fingerprint authentication solution, 2009.

[6] WEST Aquila. Wireless embedded systems technologies – L'Aquila, 2010, `www.westaquila.com`.